Classification of finitely generated abelian groups

Let G be an abelian group.

Defn: We say that G is finitely generated if there exists a finite set of elements $\{g_1, \dots, g_k\} \subseteq G$ such that

$$G = \{ m_1 g_1 + m_2 g_2 + \dots + m_k g_k \mid m_i \in \mathbb{Z} \}$$

$+$ is the group operation here

Example: 1) All cyclic groups are finitely generated abelian groups.

$$\mathbb{Z}, \quad \mathbb{Z}/m\mathbb{Z}$$

2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is not cyclic but it is generated by two elements

$(\bar{1}, \bar{0})$ and $(\bar{0}, \bar{1})$.

Non-example: S_3 is also generated by two elements $\sigma = (123)$ and $\tau = (12)$

$$S_3 = \{ e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \}$$

but is not abelian.

Structure thm for finitely generated abelian groups:

Thm: Suppose G is finitely generated abelian group.

Then $G \cong \mathbb{Z}/_{n_1\mathbb{Z}} \times \mathbb{Z}/_{n_2\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{n_r\mathbb{Z}} \times \mathbb{Z}^s$

where $n_i, s \in \mathbb{N}$,

each n_i divides n_{i+1}

and s is called rank of G.

Example: 1) For $\mathbb{Z}$, $s=1$ and $n_i = 1$.

2) If G is cyclic & finite then

$$G \cong \mathbb{Z}/n\mathbb{Z}$$

$s = 0$

3) If $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$n_1 = 2 \quad n_2 = 4$ & rank $= 0$

Qn: Classify all abelian groups of order 16.

Soln: $s = 0$

$\mathbb{Z}/16\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

and

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Qn: Classify all abelian groups of order 36.

Soln:

$$\mathbb{Z}/36\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

If $|G| = p^a$ $\quad p$ prime $\quad a \in \mathbb{N}$

Then, no of isomorphism types of G is same as number of partitions of a.

Towards a proof of Structure thm:

Let G be a finitely generated abelian group.

Defn: We say that $\{g_1, \dots, g_k\} \subseteq G$ is a basis of G if

i) $\{m_1 g_1 + \dots + m_k g_k \mid m_i \in \mathbb{Z}\} = G$

ii) $\sum m_i g_i = 0 \iff m_i g_i = 0 \ \forall i$.

Example: i) $\{1\}$ is a basis of $\mathbb{Z}$.

ii) $\{\bar{1}\}$ is a basis of $\mathbb{Z}/m\mathbb{Z}$.

iii) $\{(\bar{1}, \bar{0}), (\bar{0}, \bar{1})\}$ is a basis of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$.

Lemma: Suppose $G = \{m_1 g_1 + \cdots + m_k g_k \mid m_i \in \mathbb{Z}\}$ and suppose $(c_1, \ldots, c_k) \in \mathbb{N}^k$ such that $GCD(c_1, \ldots, c_k) = 1$.

Then, there exist generators of G $y_1, \ldots, y_k$ such that

$$y_1 = c_1 g_1 + \cdots + c_k g_k .$$

Proof: We will use induction on

$$c_1 + \cdots + c_k \in \mathbb{N}$$

If $c_1 + \cdots + c_k = 1 \Rightarrow c_i = 1$ for exactly one i and $c_j = 0$ for $i \neq j$

Then take $y_1 = g_i$, $y_i = g_1$ and $y_j = g_j$ otherwise

$\{y_1, \ldots, y_k\}$ generates G and

$$y_1 = c_1 g_1 + \cdots + c_k g_k$$

Inductive Step: Assume $c_1 + \cdots + c_k > 1$

and $c_1 \geq c_2 > 0$.

Since $\{g_1, g_2, \ldots, g_k\}$ generates G

$\{g_1, g_1 + g_2, g_3, \ldots, g_k\}$ also generates G.

Since $GCD(c_1, c_2, \ldots, c_k) = 1$

$$GCD(c_1 - c_2, c_2, \ldots, c_k) = 1$$

$$c_1 - c_2 + c_2 + c_3 + \cdots + c_k = c_1 + c_3 + \cdots + c_k$$

$$< c_1 + c_2 + \cdots + c_k$$

By induction, we know that there exists a set of generators $\{y_1, \ldots, y_k\}$ such that

$$y_1 = (c_1 - c_2) g_1 + c_2 (g_1 + g_2) + c_3 g_3 + \cdots + c_k g_k$$

$$= c_1 g_1 - c_2 g_1 + c_2 g_1 + c_2 g_2 + \cdots$$

$$= c_1 g_1 - \cancel{c_2 g_1} + \cancel{c_2 g_1} + c_2 g_2 + \cdots$$

Hence, proved.

Thm: Let G be a finitely generated abelian group. Then G has a basis, hence G is a finite direct product of cyclic groups.

Pf: We will do induction on number of generators of G.

If G has 1 generator, say g. Then $\{g\}$ is a basis for G.

Assume G has n generators. We consider all possible sets of generators of G and choose the one $\{x_1, \ldots, x_n\}$ where x_1 has smallest possible order.

Claim: $G = \langle x_1 \rangle \times \langle x_2, \ldots, x_n \rangle$

(this notation means group generated by $\{x_2, \ldots, x_n\}$)

Proof of the claim: Suppose G is not the direct product of $\langle x_1 \rangle$ and $\langle x_2, \dots, x_n \rangle$. Then, there exists a relation

$$m_1 x_1 + m_2 x_2 + \dots + m_n x_n = 0$$

where $m_1 x_1 \neq 0$; so $m_1 <$ order (x_1).

Without loss of generality, we can assume $m_i \in \mathbb{N}$.

Let $d = \text{GCD}(m_1, m_2, \dots, m_n) > 0$.

Define $c_i = m_i / d$

Then, $\text{GCD}(c_1, c_2, \dots, c_n) = 1$.

By lemma above, we know that there exists a set of generators $\{y_1, \dots, y_n\}$ such that

$$y_1 = c_1 x_1 + \dots + c_n x_n$$

$$\Rightarrow \quad d y_1 = m_1 x_1 + \dots + m_n x_n = 0.$$

but $d \leq m_1 <$ Order (x_1) $\longrightarrow\longleftarrow$

Hence, claim is proved.

Now by induction

$$G = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle.$$

There fore

$$G = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z} \times \mathbb{Z}^s$$

(p_i's need not be distinct)

Uniqueness of decomposition

Thm: s is determined inherently by G,

i.e if $G = G_1 \times \mathbb{Z}^{s_1}$ and

$$G = G_2 \times \mathbb{Z}^{s_2}$$

then $s_1 = s_2$.

Pf: Suppose

$$G = \mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_r^{a_r} \times \mathbb{Z}^s$$

Fix a prime p not equal to p_j

Consider the following map

$$\varphi : G \xrightarrow[\text{projection}]{} \mathbb{Z}^s \xrightarrow[\text{natural quotient map}]{} (\mathbb{Z}/p)^s$$

φ is a surjective group homomorphism.

$$\ker \varphi = \{ (g_1, \ldots, g_r, y_1, \ldots, y_s) \mid p \mid y_i \}$$

Further observe that p has a multiplicative inverse in $\mathbb{Z}/p_j^{a_j}\mathbb{Z}$

So, if $g_j \in \mathbb{Z}/p_j^{a_j}\mathbb{Z}$

$$g_j = p p^{-1} g_j$$

$$\ker \varphi = pG$$

By first isomorphism theorem, we know that

$$G/pG \cong (\mathbb{Z}/p\mathbb{Z})^s$$

Hence, s is determined inherently by G.

s is called Rank of G.

Suppose $G = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}$

We will now show that the primes p_i and their powers a_i are inherently determined by G.

<u>Lemma:</u> p is one of the primes p_i
$\iff$ G contains an element of order p.

pf: $\Rightarrow$: Assume that p is one of the primes p_i

So, $x = (0, 0, \ldots, p_i^{q_i - 1}, \ldots 0) \neq 0$

$p_i x = (0, \ldots, p_i^{q_i}, \ldots, 0)$
$= (0, - - , 0)$

So, x is an element of order p.

$\Leftarrow$: Suppose $x \in G$ is an element of order p.

$x = (y_1, - - , y_r) \neq 0$

but $px = (py_1, - - , py_r) = 0$

if p is not equal to any p_i, then p would have a multiplicative inverse in G, so if $py_i = 0 \Rightarrow p^{-1} p y_i = 0$
$\Rightarrow y_i = 0$

So, $x = (0, - , 0)$, but this is not possible. So $p = p_i$ for some i.

p occurs r number of times in decomposition of G i.e

$$G = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$$

$\Longleftrightarrow$ No. of elements in G of order 1 or p is p^r

$x \in \mathbb{Z}/p^n\mathbb{Z}$ has order p (or 1)

$\Longleftrightarrow \quad px \equiv 0 \pmod{p^n}$

$\Longleftrightarrow \quad x \equiv 0 \pmod{p^{n-1}}$

$\Rightarrow$ There are p elements in $\mathbb{Z}/p^n\mathbb{Z}$ of order p.

$\Longleftrightarrow$ there are p^r elements in

$$\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$$ of order 1 or p.

Similarly p^2 occurs $\underline{t}$ number of times in decomposition of G

$\iff$ there are $p^{r-t}\, p^{2t}$ elements in G of order $1, p$ or p^2.

⋮

Continue like this

So, each prime and its power that occur in decomposition of G are inherently determined by G, hence unique.

Classification of finitely generated non-abelian groups is not known yet!